UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/749,200	12/31/2003	W. Dale Hopkins	200309348-1	9964

22879 7590 10/18/2007

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
WANG, HARRIS C	

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
10/18/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/749,200	HOPKINS ET AL.	
	Examiner	Art Unit	
	Harris C. Wang	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 August 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1.

Claims 1-31 are pending

Claims 1, 8, 10, 16, 20, 24, 28, 29

Response to Arguments

Applicant's arguments filed 8/22/2007 have been fully considered but they are not persuasive.

Regarding the response to the rejection of the Claims under U.S.C. 112, the Examiner originally wrote in the first Office Action that, "The term "scanning" can be interpreted as either inputting or actually scanning an image and converting into digital data." The Applicant has chosen neither definition and amended the term "scanning" to "receiving in sequence." This amendment does not traverse the original rejection, and raises new 112 issues.

On Pages 13-14 of Applicant's Remarks, the Applicant argues "In the present case, the Examiner fails to identify reasons for connecting the secret PIN to the first input block and for connecting the non-secret identity identifier to the second input block

other than that such connection could be made. Accordingly, the Examiner uses impermissible hindsight to modify the reference into the claimed form."

The Examiner responds by pointing out that the original claim language makes no mention of "connecting the secret PIN to the first input block" and "connecting the non-secret identify identifier to the second input block." Rather the claim language, as previously presented, recites "a first cipher block in the CBC chain capable of receiving a text block derived from a secret PIN and...a second input block...capable of receiving a text block derived from a non-secret entity-identifier." The Applicant's arguments imply that there is some sort of physical connection, rather than an input block simply receiving an input number. It is unclear how a PIN can "connect" to an input block. A PIN (Personal Identification Number) is a number, and it is unclear how a number is "connected" to an input block.

The Examiner does not believe impermissible hindsight was used in the rejection of Claim 1 as the apparatus taught by Coppersmith was fully capable of receiving a PIN and a on-secret entity-identifier.

On Page 14, the Applicant argues that "Regarding Claims 4-5...Vernam does not teach first and second ciphertexts that are combined to produce a ciphertext, but rather discloses combination of a plaintext block with a ciphertext block."

This argument is unpersuasive, as the Vernam cipher works regardless of the input is "plaintext" or "ciphertext." The Vernam cipher relies on the inherent property of the exclusive-OR function, wherein the cipher can be decrypted by XOR-ing the output of the Vernam cipher with either one of the two inputs to produce the other input.

For instance:

(A XOR B) = C

C XOR A = B

C XOR B = A

Therefore to consider either one of the inputs as "plaintext" or "ciphertext" is of nominal consideration only, as either input can be used to encrypt and decrypt the other.

The Applicant then argues that "Regarding Claim 5, the combination of Coppersmith and Vernam neither describes or hints of the recovery of the secret PIN obtained from the second ciphertext block as claimed or operation in the irreversible mode."

The Examiner considers the output of a cipher block inherently "irreversible" without the proper key.

The Applicant on page 15 of the Remarks then argues "The Examiner cites the lapse of time since the discovery of pin verification (the late 1970's for IBM 3624) as motivation for making the combination. Applicants view such a lapse of time as irrelevant motivation or actually evidence against motivation since no such combination has been made since that time."

The Examiner considers adding a hexadecimal digit to decimal converter to a well known system to be obvious to one of ordinary skill in the art. Hexadecimal to decimal conversion has done well before the filing of the instant application, and one of

ordinary skill in the art could have modified the input of the IBM 3624 with a hex-to-dec converter with predictable results.

The Applicant on page 15 argues "In stating 'it would have been obvious to one of ordinary skill in the art at the time of the invention to have the processor of Matyas perform the method of Coppersmith' with the motivation that 'using a CBC using triple-DES encryption is well known in the art,' the Examiner has given absolutely no reasoning for making the combination of references, but makes an unsupported conclusion."

S.M. Matyas happens to be have been an inventor of the first reference (Matyas 4924514), as well as an author for the second reference "Triple DES Cipher Block Chaining." The Examiner considers S.M. Matyas "one of ordinary skill in the art." The Examiner believes that Matyas, would have been able to modify his invention (4924514) using his method ("Triple DES Cipher Block Chaining...").

The Applicant on page 16 argues that "Applicants dispute the obviousness of having the system of Coppersmith input a secret PIN in the first input block and input a non-secret identifier in the second input block and have the key be a PIN verification key since Matyas does not disclose application of a secret PIN and non-secret identifier to a PIN verification system."

Similar to the Examiner's earlier response, the capability of inputting a PIN and a non-secret identifier in the input of Coppersmith is considered an obvious step that would yield predictable results without requiring any modification to the system whatsoever. Furthermore, Matyas does disclose application of a secret PIN ("CPI is

a...customer selected PIN" Column 20, lines 41-45) as well as a non-secret identifier ("Validation data is a 64-bit plain user's data...Ordinarily it will be the user's PAN (personal account number) Column 20, lines 51-53).

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Where applicant acts as his or her own lexicographer to specifically define a term of a claim contrary to its ordinary meaning, the written description must clearly redefine the claim term and set forth the uncommon definition so as to put one reasonably skilled in the art on notice that the applicant intended to so redefine that claim term. *Process Control Corp. v. HydReclaim Corp.*, 190 F.3d 1350, 1357, 52 USPQ2d 1029, 1033 (Fed. Cir. 1999). The term "scanning" in claim 8 has been amended the claim to mean "receiving in sequence", while the accepted meaning is "input." The term is indefinite because the specification does not clearly redefine the term.

Claims 8, 16 and 24 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 8, 16 and 24 claim "converting hexadecimal digit ciphertext to a decimal result by scanning the hexadecimal digit ciphertext" The term "scanning" can be

interpreted as either inputting or actually scanning an image and converting into digital data.

Claim Rejections - 35 USC § 103

3.

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Claims 1-3, 7and 9 rejected under 35 U.S.C. 103(a) as being unpatentable over Coppersmith.

Regarding Claims 1-2, 7 and 9

Coppersmith teaches an apparatus comprising:

a plurality of cipher blocks linked in a Cipher Block Chain (CBC) and keyed with a Key; *(Figure 1 shows Triple-DES external feedback cipher block chaining)*

a first input block *(Figure 1, X1)* coupled to a first cipher block *(Figure 1, Y1)* in the CBC chain capable of receiving a text block.

and a second input block *(Figure 1, X2)* coupled to a second cipher block *(Figure 1, Y2)* in the CBC chain capable of receiving a text block and ciphertext from a cipher block in the CBC chain.

a logical operator that exclusive-ORs the plaintext block derived from the secret PIN with an initialization vector to produce an initialized block *(Figure 1, the Examiner interprets IV as being the initialization vector, and X1 as the plaintext block. The Examiner interprets the XORed result of IV and X1 as the initialized block);*

a first encryptor that encrypts the initialized block using 3-DES encryption to produce a first ciphertext block ; *(Figure 1. The Examiner interprets the first encryptor as the Triple-DES encryptor between X1 and Y1)*

a logical operator that exclusive-ORs the plaintext block derived from the with the first ciphertext block to produce a chained block; *(Figure 1. The Examiner interprets the first ciphertext block as Y1 and the plaintext block as X2 and the XOR in between as the logical operator)*

and a second encryptor that encrypts the chained block using 3-DES encryption to produce a second ciphertext block *(Figure 1. The Examiner interprets the second encryptor as the Triple-DES encryptor between X2 and Y2)*

Coppersmith however does not teach that the first input block that is a text block contains a secret PIN. Coppersmith further does not teach that the second input block is derived from a non-secret entity-identifier. Coppersmith does not teach that the key is a Pin Verification Key.

It would have been obvious to one of ordinary skill in the art at the time of the invention to have the system of Coppersmith input a secret PIN in the first input block and input a non-secret identifier in the second input block and have the key be a PIN verification key.

The motivation is that the system of Coppersmith without any modification can take the inputs of a secret PIN and the non-secret identifier and using a key output a Pin Verification Value.

Regarding Claim 3,

Coppersmith teaches the apparatus according to claim 2 wherein: the PIN verification apparatus operates in a reversible mode that enables recovery of the secret PIN from the second ciphertext block. In CBC it is inherent that the plaintext can be recovered by performing the reverse operations provided that the secret key is known.

Claim 4-5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Coppersmith in view of Vernam (1310719).

Regarding Claims 4 and 5,

Coppersmith teaches the apparatus according to claim 2. However Coppersmith does not explicitly teach further comprising: a logical operator that exclusive-ORs the first ciphertext block with the second ciphertext block to produce a third ciphertext block.

Vernam teaches a cipher that takes in two inputs and XORs them together to produce a ciphertext.

It would have been obvious to one of ordinary skill in the art at the time of the invention to XOR together the first and second ciphertext block to produce a third ciphertext block.

The motivation to combine is that the Vernam cipher has been a well known way to provide further encryption since 1919.

It is inherent that a PIN verification apparatus operates in an irreversible mode when the secret key is not possessed.

Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Coppersmith in view of Vernam as applied to claim 5 above, and further in view of Brachtl.

Regarding Claim 6,

Coppersmith and Vernam teach the apparatus according to claim 5. Coppersmith and Vernam do not further teach: an escrow storage coupled to the second encryptor and capable of storing the second ciphertext block.

Brachtl teaches an escrow storage coupled to a second encryptor capable of storing a second ciphertext block. *("The quantities AP KTR1 and KTR2 are stored at the issuer's data processing center enciphered under the second variant (KM2) of the issuer's master key and associated together and enclosed by the PAN for the user. The quantities PAN, PIN and KP for the user are also stored offline." Column 7, lines 49-56)*

The Examiner interprets the escrow storage as the issuer's data processing center. The Examiner interprets the storage coupled to a second encryptor as the quantities being enciphered under the second variant. The Examiner further interprets that the second ciphertext block is capable of being stored.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Coppersmith and Vernam with an escrow storage.

The motivation is firstly "for backup purposes" Column 7, line 55. The second motivation is that the reference is a patent from 1988 so therefore it has been well known to store data in an escrow storage in the PIN verification art.

Claims 8 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Coppersmith in view of Matyas.

Regarding Claim 8,

Coppersmith teaches the apparatus according to claim 1. Coppersmith does not explicitly teach: a format converter and capable of converting hexadecimal digit ciphertext to a decimal result by scanning the hexadecimal digit ciphertext, selecting a predetermined number of numeric digits, and generating output digits as a PIN Verification Value (PVV).

Matyas teaches a format converter capable of converting hexadecimal digit ciphertext to decimal result by scanning the hexadecimal digit ciphertext, selecting a predetermined number of numeric digits, and generating output digits. (Figure 9 shows a hexadecimal ciphertext input into a decimalization table. The Examiner interprets the

output digits as the PIN Verification Value. The Examiner further interprets that it is inherent that a predetermined number of digits must first be selected before converting from hex to decimal.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the PIN verification apparatus of Coppersmith with the format converter of Matyas.

The motivation is that Figure 9 describes the IBM 3624, including the format converter. This PIN verification apparatus is very well known in the PIN verification art and has been in use since the late 1970's. Therefore one of ordinary skill in the art would know to add a hexadecimal to decimal format converter to a PIN verification apparatus.

Regarding Claim 10,

Coppersmith teaches the apparatus according to claim I. Coppersmith does not explicitly teach inputs including: a length digit, x hexadecimal digits of the secret PIN, 16-(x+1) hexadecimal digits of a non-secret identifier, and a pad character for the non-secret identifier that is repeated 16- (number of digits in the non-secret identifier) times.

Matyas teaches a length digit *("a-pin-len is the number (1-16) indicating how many digits the generated PIN is assigned to the customer" Column 20, lines 53-53,* x hexadecimal

digits of the secret PIN *("CPIN is a...customer selected PIN in clear form" Column 20, lines 41-47)*, a non-secret identifier and a pad character for the non-secret identifier that is repeated 16- (number of digits in the non-secret identifier) times *("val-data, Validation data is a 64-bit plain user's data, padding included. Ordinarily it will be the user's PAN" Column 20, lines 51-53)*.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the apparatus of Coppersmith with the inputs of Mayas.

The motivation to combine is that Mayas discloses the inputs of the Generate IBM 3624 PIN process. This PIN verification apparatus is very well known in the PIN verification art and has been in use since the late 1970's. Therefore one of ordinary skill in the art would know of these inputs.

Coppersmith and Mayas do not explicitly teach a first formatter configured to construct a first incoming plaintext block from a concatenation of a length digit x hexadecimal digits of the secret Personal Identification Number (PIN) with 16-(x+1) rightmost hexadecimal digits of the non-secret entity-identifier;

and a second formatter configured to construct a second incoming plaintext block from a concatenation of y hexadecimal digits of the non-secret entity-identifier with a pad character that is repeated 16-y times.

It would have been obvious to one of ordinary skill in the art at the time of the invention to construct a first plaintext block by concatenating a length digit with x hexadecimal digits of a PIN and 16-(x+1) hexadecimal digits of a non-secret entity identifier, and to construct a second plaintext block by concatenating y hexadecimal digits of the non-secret entity-identifier with a pad character that is repeated 16-y times.

The motivation to construct the first plaintext block by concatenating a length digit with a PIN and 16-(x+1) digits is firstly because it is a plaintext block and the user can choose to input the block in any suitable format. The IBM 3624 format already includes the length digit, the PIN as well as a pad for the PIN that is 16-x in length. It would have been very obvious to one of ordinary skill to modify the IBM 3624 format to include these three inputs in a first format.

The motivation to construct the second plaintext block by concatenating y hexadecimal digits of the non-secret entity identifier with a pad character that is repeated 16-y times is that the non-secret entity identifier (val-data) already comes padded in the IBM 3624 format. Without any modification the user could, as their design choice, input the val-data into the second plaintext block as described in Coppersmith.

Claims 11-13, 16-21 and 24-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas in view of Coppersmith.

Regarding Claims 11-13,18, 20-21, 28-31

Matyas teaches a data security apparatus comprising:

an enrollment terminal capable of accepting a magnetic stripe card storing a non-secret entity-identifier and an entity-selected secret Personal Identification Number (PIN); *(Figure 3, EFT Terminal accepts a PIN and is capable of storing non secret entity identifier)*

a processor coupled to the enrollment terminal and capable of receiving the entity-identifier and the PIN; *(It is inherent that the EFT Terminal has a processor capable of receiving the entity-identifier)*

and a memory coupled to the processor *(It is inherent that the EFT Terminal has memory with code embodied on it)* and having a computable readable program code embodied therein capable of causing the processor to enroll a PIN *(Figure 3. Create PIN block)*:

a database capable of storing a plurality of PIN Verification Values (PVVs) for enrolled magnetic stripe cards; *(Figure 3, Customer Accounts Database).*

an escrow capable of storing a plurality of escrow values associated with at least some of the enrolled magnetic stripe cards; *(Figure 3, Institution Y is capable of storing escrow values)*

and a processor coupled to the database and the escrow and capable of receiving an entity-identifier, a PIN Verification Value (PVV) associated to the entity-identifier, and at least one escrow value associated to the entity-identifier; *(Figure 3,*

HPC, or the Host Processing Center inherently has a processor that is capable or receiving identifiers and values)

and a memory coupled to the processor and having a computable readable program code embodied therein capable of causing the processor to recover a PIN. *(Figure 3, The HPC and Institution Y inherently have memories capable of causing the processor to recover a PIN as shown by the Verify PIN function)*

a plurality of terminals coupled to the servers via the network *(Figure 1, EFT Terminals);*

a plurality of magnetic stripe cards enrolled in the transaction system and capable of insertion into the on-line terminals and performing transactions via the servers; *("Consider the network configuration as shown in Fig 1. The entry point at which transaction requests are intiated, such as a point of sale (POS) terminal or an automated teller machine (ATM), is defined as an EFT terminal." Column 2, lines 46-49). It is inherent that an ATM includes a plurality of magnetic stripe cards enrolled in the transaction system and capable of insertion into the online terminals and performing transactions via the servers.*

and a plurality of processors distributed among the servers, hosts, and/or the terminals, at least one of the processors being capable of executing PIN verification using a magnetic stripe card. *(Figure 1, the Host Processing center and the terminals inherently have processors, of which the processors are capable of executing PIN verification)*

means for writing the PVV to a transaction card for subsequent PIN verification *(Figure 5, shows the Remote Card Issuing Station writing PIN information to a transaction card via the Card Writer)*

Matyas does not teach a method of linking a plurality of cipher blocks, applying incoming plaintext blocks to cipher blocks, keying the cipher blocks with a key, XORing the plaintext block with an initialization vector, encrypting the initialized block using tripled DES encryptiong, XORing the plaintext block with the first ciphertext block, encrypting the chained block using triple DES encryption, and outputting the second cipher block.

Coppersmith teaches a method comprising:

linking a plurality of cipher blocks in a Cipher Block Chain (CBC); *(Figure 1 shows Triple-DES external feedback cipher block chaining)*

applying an incoming plaintext block to one of the plurality of cipher blocks; *(Figure 1 shows applying the plaintext block (X1) to a cipher block (Y1))*

applying an incoming plaintext block derived from a non-secret entity-identifier and ciphertext from a cipher block in the CBC chain; *(Figure 1 shows applying the plaintext block (X2) to a cipher block (Y2)) The Examiner interprets the X1 as the non-secret entity identifier and Y2 as the cipher block.*

keying the plurality of cipher blocks with a Key; and executing the cipher blocks resulting in generation of ciphertext (Figure 1. shows the plaintext being keyed (K1-K3) resulting in the generation of ciphertext.

exclusive-ORing the plaintext block with an initialization vector to produce an initialized block; *(Figure 1, the Examiner interprets IV as being the initialization vector, and X1 as the plaintext block. The Examiner interprets the XORed result of IV and X1 as the initialized block);*

encrypting the initialized block using triple Data Encryption Standard (3-DES) encryption to produce a first ciphertext block; *(Figure 1. The Examiner interprets the first encryptor as the Triple-DES encryptor between X1 and Y1)*

exclusive-ORing the plaintext block with the first ciphertext block to produce a chained block; *(Figure 1. The Examiner interprets the first ciphertext block as Y1 and the plaintext block as X2 and the XOR in between as the logical operator)*

encrypting the chained block using triple Data Encryption Standard (3-DES) encryption to produce a second ciphertext block; *(Figure 1. The Examiner interprets the second encryptor as the Triple-DES encryptor between X2 and Y2)*

and outputting the second ciphertext block (*The Examiner interprets the output of the second ciphertext block as supplying information)*

It is inherent that with the proper key information the original cleartext can be recovered.

It would have been obvious to one of ordinary skill in the art at the time of the invention to have the processor of Matyas perform the method of Coppersmith.

The motivation is that the method of using a CBC using triple-DES encryption is well known in the art. One of ordinary skill would be able to use the method of Coppersmith on the terminal of Matyas for the purpose of PIN encryption.

Coppersmith however does not teach that the first input block that is a text block contains a secret PIN. Coppersmith further does not teach that the second input block

is derived from a non-secret entity-identifier. Coppersmith does not teach that the key is a Pin Verification Key. Coppersmith does not teach that the output of the second ciphertext block is to be used for the purpose of PIN verification.

It would have been obvious to one of ordinary skill in the art at the time of the invention to have the system of Coppersmith input a secret PIN in the first input block and input a non-secret identifier in the second input block and have the key be a PIN verification key.

The motivation is that the system of Coppersmith without any modification can take the inputs of a secret PIN and the non-secret identifier and using a key output a Pin Verification Value. Furthermore CBC can generate ciphertext for any field. One of ordinary skill in the art would be able to take the ciphertext generated from the inputs for the purpose of PIN verification.

Regarding Claims 16 and 24,

Matyas and Coppersmith teach the method according to claim 11 and the security apparatus that invokes the method in claim 20.

Matyas teaches a format converter capable of converting hexadecimal digit ciphertext to decimal result by scanning the hexadecimal digit ciphertext, selecting a

predetermined number of numeric digits, and generating output digits. (Figure 9 shows a hexadecimal ciphertext input into a decimalization table. The Examiner interprets the output digits as the PIN Verification Value. The Examiner further interprets that it is inherent that a predetermined number of digits must first be selected before converting from hex to decimal.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the PIN verification apparatus of Coppersmith with the format converter of Matyas.

The motivation is that Figure 9 describes the IBM 3624, including the format converter. This PIN verification apparatus is very well known in the PIN verification art and has been in use since the late 1970's. Therefore one of ordinary skill in the art would know to add a hexadecimal to decimal format converter to a PIN verification apparatus.

Regarding Claims 17 and 25,

Matyas and Coppersmith teach the method according to claim 11 and the security apparatus that invokes the method in claim 20. Matyas and Coppersmith do not explicitly teach supplying hexadecimal digit ciphertext generated by a final ciphertext block in the Cipher Block Chain (CBC) as a PIN Verification Value (PVV).

It would have been obvious to one of ordinary skill in the art at the time of the invention to have the final ciphertext be in hexadecimal format.

The motivation is that hexadecimal format is well known to one of ordinary skill in the art.

Regarding Claims 19 and 27,

Matyas and Coppersmith teaches the method according to claim 11 and the security apparatus that invokes the method in claim 20.

Matyas teaches a length digit *("a-pin-len is the number (1-16) indicating how many digits the generated PIN is assigned to the customer" Column 20, lines 53-53,* x hexadecimal digits of the secret PIN *("CPIN is a...customer selected PIN in clear form" Column 20, lines 41-47)*, a non-secret identifier and a pad character for the non-secret identifier that is repeated 16- (number of digits in the non-secret identifier) times *("val-data, Validation data is a 64-bit plain user's data, padding included. Ordinarily it will be the user's PAN" Column 20, lines 51-53)*.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the apparatus of Coppersmith with the inputs of Mayas.

The motivation to combine is that Mayas discloses the inputs of the Generate IBM 3624 PIN process. This PIN verification apparatus is very well known in the PIN

verification art and has been in use since the late 1970's. Therefore one of ordinary skill in the art would know of these inputs.

Coppersmith and Matyas do not explicitly teach a first formatter configured to construct a first incoming plaintext block from a concatenation of a length digit x hexadecimal digits of the secret Personal Identification Number (PIN) with 16-(x+1) rightmost hexadecimal digits of the non-secret entity-identifier;

and a second formatter configured to construct a second incoming plaintext block from a concatenation of y hexadecimal digits of the non-secret entity-identifier with a pad character that is repeated 16-y times.

It would have been obvious to one of ordinary skill in the art at the time of the invention to construct a first plaintext block by concatenating a length digit with x hexadecimal digits of a PIN and 16-(x+1) hexadecimal digits of a non-secret entity identifier, and to construct a second plaintext block by concatenating y hexadecimal digits of the non-secret entity-identifier with a pad character that is repeated 16-y times.

The motivation to construct the first plaintext block by concatenating a length digit with a PIN and 16-(x+1) digits is firstly because it is a plaintext block and the user can choose to input the block in any suitable format. The IBM 3624 format already includes the length digit, the PIN as well as a pad for the PIN that is 16-x in length. It would have

been very obvious to one of ordinary skill to modify the IBM 3624 format to include these three inputs in a first format.

The motivation to construct the second plaintext block by concatenating y hexadecimal digits of the non-secret entity identifier with a pad character that is repeated 16-y times is that the non-secret entity identifier (val-data) already comes padded in the IBM 3624 format. Without any modification the user could, as their design choice, input the val-data into the second plaintext block as described in Coppersmith.

Claims 14 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas in view of Coppersmith as applied to claims 11 and 20 above, and further in view of Vernam.

Regarding Claims 14 and 22,

Matyas and Coppersmith teach the method according to claim 11 and the security apparatus that invokes the method in claim 20 wherein the PIN verification method is capable of operating in an irreversible mode that obstructs recovery of the secret PIN, the method comprising:

exclusive-ORing the plaintext block with an initialization vector to produce an initialized block; *(Figure 1 of Coppersmith, the Examiner interprets IV as being the*

initialization vector, and X1 as the plaintext block. The Examiner interprets the XORed result of IV and X1 as the initialized block);

encrypting the initialized block using triple Data Encryption Standard (3-DES) encryption to produce a first ciphertext block; *(Figure 1 of Coppersmith. The Examiner interprets the first encryptor as the Triple-DES encryptor between X1 and Y1)*

exclusive-ORing the plaintext block with the first ciphertext block to produce a chained block; *(Figure 1 of Coppersmith. The Examiner interprets the first ciphertext block as Y1 and the plaintext block as X2 and the XOR in between as the logical operator)*

encrypting the chained block using triple Data Encryption Standard (3-DES) encryption to produce a second ciphertext block; *(Figure 1 of Coppersmith. The Examiner interprets the second encryptor as the Triple-DES encryptor between X2 and Y2)*

and outputting the second ciphertext block (*The Examiner interprets the output of the second ciphertext block as supplying information)*

Coppersmith does not exclusively teach exclusive-ORing the first ciphertext block with the second ciphertext block to produce a third ciphertext block;

Vernam teaches a cipher that takes in two inputs and XORs them together to produce a ciphertext.

It would have been obvious to one of ordinary skill in the art at the time of the invention to XOR together the first and second ciphertext block to produce a third ciphertext block.

The motivation to combine is that the Vernam cipher has been a well known way to provide further encryption since 1919.

It is inherent that a PIN verification apparatus operates in an irreversible mode when the secret key is not possessed.

Claims 15 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas in view of Coppersmith further in view of Vernam as applied to claims 14 and 22 above, and further in view of Brachtl.

Regarding Claims 15 and 23,

Matyas, Coppersmith and Vernam teach the method and the security apparatus according to claim 14. The cited references do not further teach: storing the second ciphertext block in at least one escrow to facilitate recovery of the secret PIN.

Brachtl teaches an escrow storage coupled to a second encryptor capable of storing a second ciphertext block. *("The quantities AP KTR1 and KTR2 are stored at the issuer's data processing center enciphered under the second variant (KM2) of the issuer's master key and associated together and enclosed by the PAN for the user. The quantities PAN, PIN and KP for the user are also stored offline." Column 7, lines 49-56)*

The Examiner interprets the escrow storage as the issuer's data processing center. The Examiner interprets the storage coupled to a second encryptor as the quantities being

enciphered under the second variant. The Examiner further interprets that the second ciphertext block is capable of being stored.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Coppersmith and Vernam with an escrow storage.

The motivation is firstly "for backup purposes" Column 7, line 55. The second motivation is that the reference is a patent from 1988 so therefore it has been well known to store data in an escrow storage in the PIN verification art.

Conclusion

4.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Harris C. Wang whose telephone number is 5712701462. The examiner can normally be reached on M-F 8-5:30, Alternate Fridays Off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ R. SHEIKH can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

HCW

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100